

AMENDMENTS TO THE SPECIFICATION:

Please add the following at page 1, after the title and before line 1:

BACKGROUND

1. Technical Field

Please add the following at page 1, line 6:

2. Related Art

Please add the following at page 10, line 4:

BRIEF SUMMARY

Please amend the paragraph at page 10, beginning at line 5:

According to exemplary embodiments of the present invention there is provided a method of managing keys in a key distribution system for a communications group, the key distribution system maintaining a tree of nodes including at least one leaf node that has a parent node, each node of the group being associated with a first key,

the method comprising:

the system updating the first keys of a first branch of nodes in the tree by allocating new first keys to each of the nodes in the branch ;

the system determining an offset for generating the updated first key of each node in the branch from the previous node in the branch; and

broadcasting each of said offsets so that, given the updated first key associated with the first node of said branch, each updated first key of said branch of nodes can be calculated.

Please amend the paragraph at page 10, beginning at line 27:

The present exemplary embodiment of this invention further provides a key distribution system for a communications group, the key distribution system maintaining a tree of nodes including at least one leaf node that has a parent node, each node being associated with a first key, wherein: the first key of each parent node in the tree is derived from the first key of each of its child node by two one-way functions and a mixing function, the mixing function including an offset value as a parameter.

Please amend the paragraph at page 11, beginning at line 4:

The present exemplary embodiment of this invention also provides a key distribution system for a communications group, the key distribution system comprising an encryption key and maintaining a tree of nodes including a root node that has at least one child node, and at least one leaf node that has a parent node, the communication group comprising at least one member, wherein the encryption key comprises a join field and a leave field, and wherein:

each member of the group knows the join field of the encryption key ;

each node of the key distribution system is associated with a leave key;

the leave field of the encryption key is derived from the leave key of the root node.

Please add the following at page 11, line 26:

BRIEF DESCRIPTION OF THE DRAWINGS

Please add the following at page 12, line 22:

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

Please amend the title at page 32, before claim 1:

~~CLAIMS:~~ **WHAT IS CLAIMED IS:**